# Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 28 January 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

**Daily Overview**

- The UN News Center reports that with the unprecedented spread of bird flu in Asia raising the possibility of a human pandemic as well as a disaster for agricultural production, United Nations agencies have appealed to international donors to provide funds and technical assistance to help eliminate this global threat. (See item 21)
- SearchSecurity.com reports a new version of the dangerous Dumaru worm has surfaced and enterprise administrators are warned that this version creates a Windows Hook that logs keystrokes and opens two backdoors that experts say could enable an attacker to gain remote control of an infected system. (See item 28)
- CNN reports the U.S. East Coast is braced for another beating from the winter storms that have glazed roads, delayed flights, and caused deadly car crashes across the eastern half of the United States. (See item 30)



## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *January 27, Reuters* — **Utilities restoring power after ice storm hits the South. Progress Energy Inc. said Tuesday, January 27, crews were restoring electricity to its 83,000 customers left without power after an ice storm hit on Monday, January 26.** A

spokesperson at Progress Energy, which distributes electricity to 1.3 million customers in North and South Carolina, said **there were about 20,000 customers without service in North Carolina and about 63,000 out in South Carolina.** Elsewhere in the Carolinas, Duke Energy Corp., which distributes power to 2 million customers in North and South Carolina, said it had fewer than 8,000 homes and businesses without service. Meteorologists forecast more than a foot of snow is possible Tuesday night into Wednesday, January 28 across southern New England. New York could get as much as 6 to 12 inches of snow by Wednesday morning.
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_reuters.htm?SMDOCID=reuters_pma_2004_01_27_eng-reuters_pma_UTILITIES-RESTORING-POWER-AFTER-ICE-STORM-HITS-SOUTH&SMContentSet= 0

2. *January 27, Wired* — **Inspector general's report criticizes nuclear facility. Security guards at the country's leading nuclear storehouse have been cheating during anti-terrorism drills, according to a report released Monday, January 26, by the Department of Energy's inspector general.** Now, watchdogs in Congress and beyond are questioning whether the tons of enriched uranium at the Y-12 National Security Complex in Oak Ridge, TN, are really safe at all. Y-12 is America's main facility for processing enriched uranium. It stores nearly all of the country's reserve of about 5,000 "secondaries," the thermonuclear hearts of hydrogen bombs. When a team of Y-12 contract security guards received a perfect score during an anti-terror drill June 26, officials there were shocked. A computer model had predicted that the defenders would lose at least half of their confrontations. Officials found out the guards cheated. They had seen the computer models of the strikes the day before they were launched, rendering the test "tainted and unreliable," according to the report. **"From the mid-1980s to the present," contract security guards had been given the plans to the attacks beforehand, noted Inspector General Gregory Friedman. The defenders knew ahead of time "the specific building and wall to be attacked by the test adversary," the report noted.** Report: http://www.ig.doe.gov/pdf/ig-0636.pdf
Source: http://www.wired.com/news/politics/0,1283,62052,00.html?tw=w n_tophead_1

[Return to top]

## Chemical Sector

3. *January 27, Coshocton Tribune (Ohio)* — **Truck carrying aqua ammonia struck by car, I-71 closed.** Part of Interstate 71 in Ohio was closed in both directions Monday after a car hit a commercial truck, causing it to overturn and spill aqua ammonia, the Ohio Highway Patrol said. Patrol and chemical cleanup crews closed more than 15 miles of I-71, from U.S. Route 30 to state Route 539 on Monday afternoon. U.S. Route 250 also was closed in both directions while an unknown amount of ammonia was cleaned up. The truck was heading northbound on I-71 in Ashland when it was struck early Monday afternoon, went off the road and overturned, the Ohio Highway Patrol said. There were no serious injuries. Wintry weather did not appear to be a factor in the accident, authorities said. **Aqua ammonia, also known as ammonium hydroxide, is often used in fertilizer, refrigerants or home cleaning products. Exposure to the chemical can cause breathing problems and throat or eye irritation.**
Source: http://www.coshoctontribune.com/news/stories/20040127/localn ews/301738.html

[Return to top]

## Defense Industrial Base Sector

4. *January 26, Navy News Stand* — **U.S. Naval Forces Southern Command relocates to Florida. The Navy has decided to relocate U.S. Naval Forces Southern Command (USNAVSO) from Naval Station Roosevelt Roads, Puerto Rico, to Naval Station Mayport, FL.** On September 30, the President of the United States signed into law the Fiscal Year 2004 Defense Appropriations Act. The legislation included language that calls for the Navy to close U.S. Naval Station Roosevelt Roads no later than six months after enactment of the Act. The Navy studied a number of locations and took into account availability of existing infrastructure, communications capabilities, and anti−terrorism/force protection support, amongst other factors. This relocation is scheduled to commence next month, and be completed by March 2004. Initially, Commander, U.S. Naval Forces Southern Command will be "dual−hatted" with Commander Naval Surface Group 2, and the two staffs will be consolidated.
Source: http://www.news.navy.mil/search/display.asp?story_id=11557

[Return to top]

## Banking and Finance Sector

5. *January 27, The Star (Malaysia)* — **RHB Bank warns of e−mail scam. RHB Bank in Malaysia has issued a warning about fake or spoof e−mail sent by fraudsters trying to obtain customers' logins and passwords by tricking them into visiting a fake Website.** Several RHB Bank customers in Malaysia received authentic−looking e−mail purportedly sent by RHB Bank, but which are actually fake. The fake e−mail has the subject header "!your account − RHB Bank" and is supposedly from "RHB BANK." "RHB Bank did not send this e−mail, and we did not authorize it," said an RHB spokesperson. **The spoof e−mail urges customers to check the balance in their RHB Bank account by surfing to a valid−looking web address, but those who do so are directed to a fake Website.** Such spoof e−mail and fake Websites are not new, but these scams have become increasingly common in recent months. This practice is popularly known as "phishing" among scammers, and it is also one of the aspects of "social engineering," a term that describes non−technical methods used to gain access to bank accounts, passwords, and other privileged information.
Source: http://star−techcentral.com/tech/story.asp?file=/2004/1/27/technology/7191682&sec=technology

6. *January 26, Computerworld* — **Bank group offers guidelines on outsourcing security risks. A consortium of the country's top financial services firms has published a set of industry guidelines to use in evaluating the security risks of IT outsourcing deals.** The Banking Industry Technology Secretariat (BITS) released the security guidelines as an addendum to an existing framework for managing business relationships with IT services providers. **The group's goal is to help financial services firms streamline the outsourcing evaluation process and better manage the risks of handing over control of key corporate systems to vendors.** The guidelines are based on ISO 17799 code of practice for information security management, which covers categories such as documenting corporate security policies and classifying assets. Bob Cedergren, second vice president of information security and business

continuity planning at Fortis Inc., a financial services firm with U.S. operations in New York, said security concerns related to outsourcing are getting more attention in corporate boardrooms. "Each time there's a virus outbreak, this gets discussion within our CIO group here at Fortis as well as with the CEOs" of individual business units, Cedergren said. The BITS guidelines, which are built into a 33−page spreadsheet, provide a single set of rules for evaluating outsourcing and IT services vendors, Cedergren said. Additional information available on the BITS Website: http://www.bitsinfo.org/
Source: http://www.computerworld.com/managementtopics/outsourcing/story/0,10801,89381,00.html

[Return to top]

## Transportation Sector

7. *January 27, Transport Topics News* — **TRB panel asks government to coordinate freight data. The government should coordinate freight data collection in the United States because information on freight movement is needed to help public agencies make decisions about highway infrastructure, safety and security, economic competitiveness and environmental issues,** a report by the Transportation Research Board (TRB) said. The deputy director of the Department of Transportation's Bureau of Transportation Statistics, Richard Kowalewski, said BTS "endorses" development of a national freight−data program. “There is a strong consensus that freight is driving the economy,” Kowalewski said in a telephone interview with Transport Topics. “There just hasn’t been a lot of freight planning at the state, local or national level [because] people felt there was a lack of data upon which to base decisions.”
Source: http://www.ttnews.com/members/topnews/0011068.html

8. *January 27, Government Technology* — **Las Vegas pilots eye−scan drug testing. The Las Vegas Division of the Nevada Department of Parole and Probation launched a pilot program to test eye−scan technology called PassPoint.** The system requires no urine, and uses a 30−second self−administered test with immediate results. Pass Point detects and identifies eight different categories of drugs, including marijuana, depressants, opiates, stimulants and inhalants. The offenders check in to test and enter their personal ID number, based upon their initial baseline test, which is a "clean" or drug−free test. **This baseline establishes the unique data that positively identifies offenders each time they test, with no chance of faking their identity.** The person looks into a machine and observes a series of 30−second light displays which measure "nystagmus" or eye movement, which indicates specific categories of drugs. Nationally over one million screens have been performed since 2000, saving hundreds of thousands of dollars annually while increasing offender supervision and public safety.
Source: http://www.govtech.net/news/news.php?id=86149

9. *January 27, Department of Transportation* — **Secretary Mineta calls for action to end future gridlock in the skies.** Department of Transportation Secretary Norman Y. Mineta today, January 27, announced plans for a new, next generation air transportation system with expanded capacity to relieve congestion, prevent gridlock and secure America's place as global leader in aviation's second century. In a speech before the Aero Club of Washington, DC, the

Secretary warned that recent delays at Chicago's O'Hare airport marked the return of increased passenger demand for air travel and potential gridlock in the skies. **He said that the Federal Aviation Administration has set in motion several airspace modernization plans to add capacity and improve efficiency, including seven new air traffic control towers; five new terminal air traffic control facilities; new advanced radar systems at 12 airports; and the state−of−the−art STARS air traffic control system at 14 airports.** He added that seven airports are building new runways and four major hub airports −− Boston, Charlotte, Denver and Minneapolis −− will be getting advanced weather satellite/radar systems to minimize weather−related delays. The Secretary said the Administration's initiative would bolster technology aimed at tripling airspace capacity, modernizing GPS navigation and enhancing on−board technologies to maximize passenger and aircraft safety.
Source: http://www.dot.gov/affairs/dot0404.htm

**10.** *January 27, Department of Transportation* — **Trucker calls focused on compliance.** An initial review released today, January 27, shows that truckers contacting the Federal Motor Carrier Safety Administration (FMCSA) are committed to following new hours−of−service rules, but still have questions about changes made to the 60−year old regulations. **The review is based on thousands of calls from commercial drivers made to the FMCSA,s 24−hour, toll−free help line established to answer questions about the new hours−of−service rule implemented January 4.** Help line personnel have answered almost 5,500 calls from truckers wanting to understand the new rule. Initial call tracking reports indicate the majority of questions asked concern the sleeper−berth exemption, the 34−hour restart provision, the definition of a 14−hour workday, and procedures for recording hours in driver logbooks. "Despite some dramatic predictions about the impact of the new rules, drivers are telling us they are working to comply," said FMCSA Administrator Annette M. Sandberg.
Source: http://www.dot.gov/affairs/fmcsa203.htm

**11.** *January 27, The Clarion−Ledger (Mississippi)* — **Though Amtrak has most passengers ever, it faces uncertain future.** Last year more travelers climbed aboard Amtrak than ever before, but supporters still expect a bumpy ride over continuing federal subsidies. Company President David Gunn credits lower fares, restructured routes and more convenient schedules for helping draw 600,000 new travelers, a nearly three percent rise over 2002. **But he said the reason Amtrak should top 25 million riders this year has as much to do with traffic jams and air security checkpoints as with changes he has made. "The basic congealing of airports and highways has driven people to us," Gunn said.** "As the system gradually grinds to a halt, you only need a small increment of people to say: 'I've had it. I'm going to take the train,' for that to have a big impact on us." **In his effort to run a back−to−basics railroad company, he's restructured routes and ticket prices, eliminated administrative positions, beefed up production lines at maintenance shops and abandoned the company's unprofitable venture in freight shipping.** The result: Amtrak finished its last quarter $40 million under budget.
Source: http://www.clarionledger.com/news/0401/26/b02.html

**12.** *January 27, The Honolulu Advertiser* — **Midway airport financed through September.** Congress' approval of the federal budget last week provided secure financing for the operation of Midway Atoll's airport, keeping it available for emergency landings like that of a Continental Airlines jet January 6 with 294 people on board. **The U.S. Fish and Wildlife Service, which**

**operates the Midway Atoll National Wildlife Refuge, has been keeping the airfield open with emergency money provided on a month−by−month basis while awaiting a long−term source of revenue.** The service had been within days of closing the field when the Continental flight from Japan to Texas developed an oil leak in one of its two engines. It put down at Midway and stayed there to await the arrival of repair crews and spare parts. Sen. Dan Inouye, D−Hawaii, announced that the federal Department of Transportation would provide $3.2 million to keep the airport running through the end of the federal fiscal year on September 30. "The emergency landing earlier this month, which ensured the safety of the nearly 300 people on board, dramatically underscores the importance of this runway," Inouye said in a news release. "Midway currently serves as the only emergency landing facility in this region of the Pacific."
Source: http://the.honoluluadvertiser.com/article/2004/Jan/27/ln/ln2 8a.html

13. *January 26, Associated Press* — **California man sentenced in airport threat.** A California man who threatened to blow up a terminal at Dallas−Fort Worth International Airport was sentenced Monday, January 26, to one and a half years in prison. **Deshon Lamar Brown, 19, of Long Beach, CA, had pleaded guilty in October to making a threat to destroy a building by fire and explosion. In addition to the prison sentence, Brown was ordered to make $4,000 in restitution.** Prosecutors said Brown admitted using his cell phone to place a number of calls to police in July, telling them he was at the airport, had walked past a police officer, had placed a bomb inside a bathroom at the Delta terminal, was going to start shooting people in a ticket line and that the explosives were in a car. Brown had no explosives and told authorities he made the calls because he enjoyed watching police respond to the calls, prosecutors said. Brown was ordered to surrender to the Bureau of Prisons on February 23.
Source: http://www.dfw.com/mld/startelegram/news/state/7804027.htm

[Return to top]

## Postal and Shipping Sector

Nothing to report.
[Return to top]

## Agriculture Sector

14. *January 27, Oster Dow Jones Commodity News* — **USDA says BSE investigation nearing an end.** The U.S. Department of Agriculture's (USDA) investigation into tracing and testing cattle associated with the Washington state dairy cow diagnosed with bovine spongiform encephalopathy (BSE) is nearing an end, said Ron DeHaven, deputy administrator of veterinary services, for the USDA's Animal and Plant Health Inspection Service. **An international review team composed of BSE experts from around the world told USDA investigators as it reviewed the U.S. response to the case of BSE that it needed to focus on 25 of the 81 cows sent in a shipment of cows from Canada that included the cow that tested positive, DeHaven said.** These cows are ones that were born a year before and a year after the sick cow. A full report from the review team is expected "in a couple of weeks," DeHaven said. Taking into account normal culling practices of U.S. dairy producers and an assumed rate of lost

identification, the review team would expect investigators to be able to locate 11 of those 25 cows, DeHaven said. They were surprised that investigators had located 14. **At some point, looking for a positive identification of the rest of the 25 cattle reaches a point of diminishing returns, DeHaven said. Researchers could look for months and never identify them all positively.**
Source: http://www.cropdecisions.com/show_story.php?id=23271

15. *January 27, China Daily* — **China confirms bird flu. China has become the latest country in Asia to report infections of bird flu, after a state−level laboratory confirmed on Tuesday that some poultry had died from the H5N1 strain in its southwestern province of Guangxi, bordering Vietnam.** Some chickens and ducks raised in southern China's Hunan Province and central China's Hubei Province also died over the weekend, China's Central Television Station (CCTV) reported. On January 23, some ducks raised by a farmer in Dingdang Town, Long'an County, Guangxi, fainted and later died. Initial testing by the local medical department said the poultry possibly died from the bird flu. State laboratories are now testing samples sent by Hunan's Wugang City, and Hubei's Wuxue City. Chickens and ducks raised there were also killed. Local veterinary departments preliminarily diagnosed the cause of the death as the H5N1 strain of bird flu.
Source: http://www1.chinadaily.com.cn/en/doc/2004−01/27/content_3011 72.htm

16. *January 25, Associated Press* — **Captive elk tests positive for wasting disease. A Colorado ranch previously linked to chronic wasting disease (CWD) has been quarantined because a four year old captive bull elk has tested positive for the disease.** The infected elk was from the a ranch south of Craig, where 10 wild mule deer trapped behind the ranch's fences were found to be infected two years ago. The latest case was the first positive test identified in a captive elk in two years. **Colorado has quarantined the 200 elk at the ranch.** "But it is the top priority of this agency to put that herd down," Colorado Department of Agriculture spokesman Jim Miller said. After the infected mule deer were found two years ago, the ranch owner refused to let the state kill the elk and test them for signs of infection. Agriculture officials declined to mount a legal battle to force his hand. The new case involved a bull that was killed by other elk at the ranch. Researchers say infected animals often provoke an aggressive response from herdmates.
Source: http://www.trib.com/AP/wire_detail.php?wire_num=82183

[Return to top]

## Food Sector

17. *January 27, Honolulu Advertiser* — **Crack in wheat silo prompts evacuation. A large crack in a 100−foot Hawaiian flour mill silo that contained 1,250 tons of wheat forced the evacuation of businesses surrounding the Nimitz Highway mill Monday.** The crack and bulge in the concrete silo were discovered early Monday morning. The mill is near Pier 24 and is surrounded by many businesses. By 11:30 a.m., workers were told to leave. "What they were worried about is the concrete from the (collapsed) silo somehow gaining velocity, going across the roadway and puncturing one of the fuel holding tanks," said Honolulu Fire Department Capt. Kenison Tejada. He said there also was a concern that the particles from the silo could cause a dust explosion.

Source: http://the.honoluluadvertiser.com/article/2004/Jan/27/ln/ln2 4a.html

18. *January 26, Food and Drug Administration* — **Expanded BSE safeguards announced.** Health and Human Services (HHS) Secretary Tommy G. Thompson on Monday, January 26, announced several new public health measures, to be implemented by the Food and Drug Administration (FDA), to strengthen significantly the multiple existing firewalls that protect Americans from exposure to the agent thought to cause bovine spongiform encephalopathy (BSE) and that help prevent the spread of BSE in U.S. cattle. **Specifically, HHS intends to ban from human food (including dietary supplements), and cosmetics a wide range of bovine−derived material so that the same safeguards that protect Americans from exposure to the agent of BSE through meat products regulated by the U.S. Department of Agriculture also apply to food products that FDA regulates.** FDA will also prohibit certain currently allowed feeding and manufacturing practices involving feed for cattle and other ruminant animals. FDA will publish two interim final rules that will take effect immediately upon publication.
Source: http://www.fda.gov/bbs/topics/news/2004/hhs_012604.html

19. *January 26, FoodNavigator.com* — **Basil and thyme combat foodborne bacteria. New research into basil and thyme essential oils reveals their ability to curb Shigella, a harmful foodborne bacteria.** Previous research has shown that thyme and basil have antimicrobial potential. Building on this research, scientists at Ghent university in Belgium opted to investigate the antimicrobial impact of thyme and basil essential oil and their major constituents towards Shigella. According to the researchers, thyme essential oil and its major constituents thymol and carvacrol decontaminated Shigella innoculated lettuce. They also found that thyme and basil essential oil, and their major compounds thymol, estragol, carvacrol, linalool, and p−cymene, inhibited Shigella in an agar diffusion method. **"In this study, it was shown that essential oils and their compounds have potential to be used for decontamination of minimally processed vegetables,"** the researchers said.
Source: http://www.foodnavigator.com/news/news−NG.asp?id=49337

[Return to top]

## Water Sector

20. *January 27, St. Petersburg Times* — **Reclaimed water is the key to plan. Some 30,000 people could be in line to get reclaimed water in the next decade under a plan endorsed Monday, January 26, by Tampa Bay Water and the Southwest Florida Water Management District. The plan would also produce an extra fourteen million gallons of drinking water for the region by 2012, without tapping the underground aquifer, Tampa Bay Water officials say.** Engineers estimate that all the pipes and pumps needed to make the plan work will cost about $300−million. The two water agencies and the region's local governments would pay the bills using money from water ratepayers and taxpayers. Tampa Bay Water is pursuing a plan to draw fourteen million gallons of drinking water a day from the Alafia and Hillsborough rivers and the Tampa Bypass Canal. The utility would replace what it takes out of the canal or rivers with treated wastewater from Tampa's sewer plant. The wastewater would be put into the waterways so the flow into Tampa Bay would not be harmed. No wastewater would mix with drinking water.

Source: http://www.sptimes.com/2004/01/27/Hillsborough/Reclaimed_wat er_key_t.shtml

[Return to top]

## Public Health Sector

21. *January 27, UN News Center* — **UN agencies call for aid to prevent bird flu becoming global threat. With the unprecedented spread of bird flu in Asia raising the possibility of a human pandemic and causing disaster for agricultural production, United Nations agencies Tuesday appealed to international donors to provide funds and technical assistance to help eliminate the global threat, including the mass killing of infected birds.** The possible widespread occurrence of highly pathogenic avian influenza in several areas in Asia represents a significant control challenge, the UN Food and Agriculture Organization (FAO) and World Health Organization (WHO) said in a joint statement with the World Organization for Animal Health (OIE). **To date only two countries, Vietnam and Thailand, have reported laboratory confirmed cases of bird flu infection in humans, the first with seven cases, six of them fatal, the second with three cases, two of them fatal.** But, the three agencies warned, "Although it has not happened yet, the bird flu presents a risk of evolving into an efficient and dangerous human pathogen." **If the virus circulates long enough in humans and farm animals, there is an increased risk that it may evolve into a pandemic influenza strain which could cause disease worldwide, they added.**
Source: http://www.un.org/apps/news/story.asp?NewsID=9580&Cr=bird&Cr 1=flu

22. *January 27, Asia Pacific News* — **Malaysia adopts SARS measures to keep out bird flu.** Malaysia is adopting measures used to combat Severe Acute Respiratory Syndrome (SARS) to protect its people and poultry industry against any possible outbreak of bird flu. Health Minister Chua Jui Meng said it was due to this high level of surveillance, including tighter border checks, that the country has not seen any case of avian influenza. With several Asian nations falling victim to the bird flu virus, Malaysia is bracing itself against a possible onslaught of the disease. **The national surveillance machinery set up during the SARS outbreak last year is being used to keep the country safe from bird flu. Chua said these measures also helped keep the number of flu cases among humans down.** To protect both the people and poultry business, all poultry imports from affected countries have been banned. Malaysia has also sealed its borders to prevent any smuggling of live chicken or chicken products from Thailand and Indonesia. **Although the World Health Organization has yet to issue any travel advisory, the Malaysian government has urged tourists visiting affected countries to stay away from livestock markets and poultry farms to avoid possible infections. Those developing flu like symtoms were asked to seek immediate medical attention at local government hospitals.**
Source: http://www.channelnewsasia.com/stories/southeastasia/view/68 182/1/.html

[Return to top]

## Government Sector

Nothing to report.

[Return to top]

## Emergency Services Sector

**23.** *January 27, The Sedalia Democrat (Missouri)* — **Official: Hospitals not ready for attacks. Missouri may be better equipped to prevent and respond to terrorist attacks than in September 2001, but it still has a long way to go, said Col. Tim Daniel, Missouri's homeland security director,** on Monday, January 26. In particular, the retired 28−year Army veteran was concerned with the treatment of victims following an attack by weapons of mass destruction. **In the case of a biological attack, "This region's hospitals could not take the load," Col. Daniel said. "We do not want to be in a situation where CNN is out front of locked hospital facilities showing Americans not being able to get treatment because there is no room in the inn."** Col. Daniel spoke at a homeland security summit called by U.S. Rep. Ike Skelton, D−Lexington, whose 4th District includes Pettis County. Some 104 city, county and state police, fire, emergency management and health officials gathered at Central Missouri State University to participate in the four−hour event.
Source: http://www.sedaliademocrat.com/News/288680856568995.htm

[Return to top]

## Information and Telecommunications Sector

**24.** *January 27, Indiana Digital Student* — **Campus Website hacked. Five hours after this year's biggest snowstorm had stopped, Indiana University (IU) was put under an emergency alert, caused by a student hacker who manipulated the campus warning Website.** IU spokesperson Jane Jankowski said the server of the emergency Website did not have adequate security and that it had been breached from the outside by a student on the IU campus. Students visiting the Website were greeted with the incorrect emergency alert and a plea to "call up your congressman and suggest the educational process at Indiana University be suspended on Monday." The site also directed students to the National Weather Service and the Drudge Report Web sites "for details." Jankowski said the incorrect information was fixed on Monday, January 26. She said since then, **the hole in security has been fixed, and the site is no longer vulnerable to such unauthorized access. Jankowski said the student hacker has been caught and referred to the dean of students for reprimand.**
Source: http://www.idsnews.com/story.php?id=20854

**25.** *January 27, CERT/CC* — **CERT Advisory CA−2004−02: Email−borne Viruses.** Over the past week, two more mass−mailing viruses, W32/Bagle and W32/Novarg, have impacted a significant number of home users and sites. The technology used in these viruses is not significantly different from prior mass−mailing viruses such as W32/Sobig and W32/Mimail. Unsolicited email messages containing attachments are sent to unsuspecting recipients. They may contain a return address, a provocative envelope, or something else that encourages its receiver to open it. This technique is called social engineering. **The widespread impact of these latest viruses, which rely on human intervention to spread, demonstrates the effectiveness of social engineering**. It continues to be important to ensure that anti−virus software is used and updated regularly, that attachments are examined on mail servers, and that

firewalls filter unneeded ports and protocols.
Source: http://www.cert.org/advisories/CA−2004−02.html

**26.** *January 27, Federal Computer Week* — **New worm avoids feds for now. A new mass−mailing computer worm that began rapidly spreading throughout the Internet Monday, January 26, apparently avoids targeting the e−mail addresses of government agencies, military facilities and large software companies**, according to a security expert at a leading anti−virus firm. The worm−−known as MyDoom, W32.Novarg.A@mm, Shimgapi or as a variant of the MiMail worm−−is an encrypted program that creates a mass−mailing of itself, which may clog mail servers or degrade network performance. By avoiding federal sites and large software companies, **the worm's author could be "attempting to get lead time before anti−virus definitions" are written to block the worm**, said Alfred Huger of Symantec Corp. If the worm started attacking .mil and .gov e−mail addresses as well as antivirus vendors, then signatures could be written to thwart it much sooner, he said.
Source: http://www.fcw.com/fcw/articles/2004/0126/web−virus−01−27−04 .asp

**27.** *January 26, The Register (UK)* — **Over 400 scammers are working the phones. Nigerian scammers increasingly are calling U.S. companies on the phone, using relay phone services. These are normally free calls made by supposedly deaf people using keyboards which go to a phone company operator, who places a phone call and speaks for them.** Companies offer these services at no cost. The scams can take several forms, experts say. Very often, scammers order goods with fraudulently obtained credit cards and have them shipped to Africa. They tell their victims it is a rush job that must be in the hands of the air freight company within hours. **The orders have several characteristics. The scammers often type in all caps and their English is poor. They usually want fast shipment (with shipping cost no objection) and most orders are huge in size. Most favorable are commodity item that can be quickly resold.** Never trust Internet relay calls unless you actually know the person calling you, a "worn out relay operator" warns.
Source: http://www.theregister.co.uk/content/6/35104.html

**28.** *January 26, SearchSecurity.com* — **Worm opens two backdoors, logs keystrokes. A new version of the dangerous Dumaru worm has surfaced and enterprise administrators are warned that this version creates a Windows Hook that logs keystrokes and opens two backdoors that experts say could enable an attacker to gain remote control of an infected system.** Dumaru−Y can be contained, however. The worm travels compressed in a zip file as a .exe file. Blocking these executables and others that have no business merit should prevent infections. Most administrators have adopted this as a best practice. **The worm affects Windows Server 2003, Windows 2000, NT, XP, 98, 95 and ME systems via an e−mail with the subject line: "Important information for you. Read it immediately !" The message promises photos of a woman and the attachment is called "myphoto.jpg.exe. It is important to note that there are 56 spaces between .jpg and .exe in the attachment's file name**. If executed, the worm searches files on the hard drive for e−mail addresses to mail itself to potential new victims via a self−contained SMTP engine. It also creates a WindowsHook, which according to Microsoft is a tool that intercepts messages, keystrokes, mouse actions and other events before they reach an application. The worm also starts an infinite loop looking for an Internet connection from the infected computer. **More specifics can be found at he Sophos website**: http://www.sophos.com/virusinfo/analyses/w32dumaruy.html

Source: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci946167,00.html

**Internet Alert Dashboard**

**Current Alert Levels**

| | |
|---|---|
| AlertCon: 2 out of 4<br>https://gtoc.iss.net | Security Focus ThreatCon: 2 out of 4<br>http://analyzer.securityfocus.com/ |

**Current Virus and Port Attacks**

| | |
|---|---|
| **Virus:** | #1 Virus in the United States: **WORM_MIMAIL.R**<br>Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States] |
| **Top 10 Target Ports** | 6129 (dameware), 1434 (ms−sql−m), 135 (epmap), 137 (netbios−ns), 1433 (ms−sql−s), 445 (microsoft−ds), 80 (www), 139 (netbios−ssn), 901 (realsecure), 23 (telnet)<br>Source: http://isc.incidents.org/top10.html; Internet Storm Center |

[Return to top]

# General Sector

**29.** *January 27, Associated Press* — **Libya nuclear components arrive in U.S.** An American plane carrying components of Libya's nuclear weapons and missile programs arrived Tuesday in the United States as Libya's president, Moammar Gadhafi, follows through on a pledge to dismantle the program. **The plane landed at McGhee Tyson airport outside Knoxville, TN, carrying about 55,000 pounds of equipment, including stock to enrich uranium, centrifuge parts, and guidance sets for long−range missiles,** White House spokesman Scott McClellan said. The equipment likely will be evaluated at the Oak Ridge nuclear weapons plant in Tennessee. The "most sensitive documentation" associated with Libya's nuclear program arrived by plane last week, McClellan said. **Also, McClellan announced that Libya had begun destroying chemical munitions.** The White House gave no indication it was ready to ease the U.S. economic sanctions on Libya, nor did the State Department say Libya's designation as a supporter of terrorism would be canceled. **McClellan said the shipments were "only the beginning of the elimination of Libya's weapons."**
Source: http://story.news.yahoo.com/news?tmpl=story&cid=515&ncid=721&e=9&u=/ap/20040127/ap_on_re_af/us_libya

**30.** *January 27, CNN* — **Heavy snow forecast for New England. The U.S. East Coast braced Tuesday, January 27, for another beating from the winter storms that glazed roads, delayed flights and caused deadly car crashes across the eastern half of the United States.** The storms are to blame for at least 38 deaths from the Midwest to the Atlantic Coast,

according to The Associated Press. While improving conditions are expected in the Midwest, icy peril will continue for the Middle Atlantic and New England states, forecasters said. A storm brewing off the North Carolina coast is heading inland and north and could dump as much as 14 inches of snow in New England, said Donald Miller, a National Weather Service operational support meteorologist. "Snow amounts will range from 6 to 14 inches, with lower amounts around Cape Cod and Hyannis and the coasts," Miller said. "But in eastern New York and northeastern Pennsylvania the amount could approach 15 inches in some spots." **Earlier in the day, airports in Illinois, North Carolina and New York reported weather−related delays up to two hours because of ice and fog. Those waits now average about 30 minutes. In South Carolina, where 150,000 customers lost electricity overnight, officials have recorded six weather−related traffic deaths, the top single−state total from the storm.**
Source: http://www.cnn.com/2004/WEATHER/01/27/sprj.ww04.winter.storm /index.html

31. *January 26, Star Bulletin (Honolulu, HI)* — **Tornadoes whirl in Hawaii . Tornadoes touched down in Central Oahu on Sunday, January 25, as unstable weather produced heavy rain, thunder and lightning throughout the islands.** Storms on the Big Island brought heavy rain, flooding and hail of up to an inch in size, according to a Civil Defense official. Three Oahu tornadoes were reported in the Kunia area, according to National Weather Service lead forecaster Ray Tanabe. "It did appear that there was a tornado. It was a visible dust cloud that reached all the way to the surface," said Tanabe. The unusual funnel clouds drew the attention of residents. "It started to connect from the top, and it disappeared. It started to form again from the bottom," said Ewa Beach resident Regina McAnulty, who grabbed her camera to take pictures of the tornado after she saw it forming about 2 p.m. Both ends of the dust cloud connected for less than a minute, said McAnulty. **Heavy showers were scattered across Oahu on Sunday, prompting flash flood warnings until 10 p.m. for central and windward parts of the island as a stationary band of thundershowers unloaded in the Koolau Mountains above Kaaawa and Waikane**. All islands were under a flash flood watch until 4 a.m. on Monday, January 26. The sudden thunderstorms formed after heat rising from the central plains merged with unstable weather moving in, said Tanabe.
Source: http://starbulletin.com/2004/01/26/news/story2.html

[Return to top]

**DHS/IAIP Products &Contact Information**

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

## DHS/IAIP Daily Open Source Infrastructure Report Contact Information

| | |
|---|---|
| Content and Suggestions: | nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703)883−3644 |
| Subscription and Distribution Information | Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−3644 for more information. |

## Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call (202)323−3204.

## DHS/IAIP Disclaimer